REMARKS

April 5, 2011 Interview

The undersigned, David C. Kellogg, thanks the Examiner and Primary Examiner Zhia for the telephone call of April 5, 2011 discussing the above-identified patent application.

During the telephone call, the Examiners agreed to reopen prosecution and issue a new Office Action, which would reset the six month statutory period initiated by the November 5, 2010 Office Action.

In the telephone call, the Examiner's also suggested that the broadest reasonable interpretation of the "identity-based-encryption (IBE) private key of a user," as recited in claim 13, included master secret s of Gentry. Applicant respectfully disagrees.

A master secret is not the same as a private key. Gentry discloses that users' private keys are generated and distributed by a private key generator using a master secret. Users, in Gentry, use their private keys in cryptographic exchanges. If a user was provided with the master secret, the cryptographic exchanges between users would no longer be secure and Gentry's system would be useless. The suggestion that master secret s of Gentry is equivalent to applicant's IBE private key of a user is therefore not consistent with the

interpretation that those skilled in the art would reach (and is not consistent with applicant's specification), as required by M.P.E.P. §2111.

The statement relied upon in the rejection, in which it was suggested that "Gentry does disclose using an IBE private key to compute a public key," was also discussed. The undersigned pointed out that Gentry discloses computing a public key P_A for a user by apply a hash function to the user's identity ID_A. However, Gentry's master secret s and private keys (e.g., S_A) are not used in computing Gentry's public keys. For at least these reasons, Gentry does not disclose "using the IBE private key to compute... a commitment" (keeping in mind that applicant's IBE private key was suggested to be either Gentry's master secret S or one of Gentry's private keys and that applicant's commitment was suggested to be Gentry's public key). The Examiners agreed, during the April 5, 2011 telephone call, that col. 5, lines 5-25 of Gentry does not disclose these features.

For at least these reasons, claim 13 is patentable over Gentry and Deng, even if these references are combined. Claims 14-17 depend from claim 13 and are allowable at least because claim 13 is allowable.

Conclusion

The foregoing demonstrates that claims 1-19 are in condition for allowance. Reconsideration and allowance of the application are respectfully requested.

The Commissioner is hereby authorized to charge any fees due in connection with this submission to Deposit Account No. 502942.

Respectfully submitted,

Date: April 5, 2011

/David C. Kellogg/
David C. Kellogg
Reg. No. 62,958
Telephone: 415-837-0659
Agent for Applicant
Customer No. 36532